configured to prevent access to the audio streams, respectively, by the unauthorized software applications;

receive process identifier data from at least one software application requesting to access one of the plurality of audio streams;

determine whether the at least one software application requesting access to the audio stream is an unauthorized software application; and

control the respective software driver to prevent access to the audio stream by the determined unauthorized software application.

13. A non-transitory computer readable medium storing computer executable instructions for preventing unauthorized access to audio data, including instructions for:

storing, in a data buffer by an audiodg.exe process, the audio data received from an audio endpoint device;

installing, in a memory of a computer, a software driver associated with an audio session, the software driver being configured to prevent access to the audio data by unauthorized software applications;

receiving process identifier data from a software application requesting to access the audio data stored in the data buffer;

determining whether the software application requesting access to the audio data is an unauthorized software application based upon the process identifier data, wherein the unauthorized software application comprises an application having at least one process that is identified as untrusted, malicious, or not authorized by a user to access the audio data;

controlling the software driver to prevent access to the audio data by the determined unauthorized software application; and

converting the audio data to zeroes when the software application requesting access to the audio data is determined to be an unauthorized software application based on received process identifier data.

14. The non-transitory computer readable medium of claim **13**, further comprising instructions for monitoring for and intercepting requests from the software application to access the audio data stored in the data buffer.

15. The non-transitory computer readable medium of claim **13**, wherein the instructions for determining of whether the software application requesting access to the audio data is an unauthorized software application comprises at least one of:

monitoring activities of the requesting software application to determine whether the software application is trusted or not trusted;

scanning the requesting software application by accessing a database of signatures of known viruses and comparing a signature of the requesting software application; and

receiving, from a user, a command whether to grant access to the audio data by the requesting software application.

16. The non-transitory computer readable medium of claim **13**, further comprising instructions for:

directly storing the audio data received from the audio endpoint device in the data buffer; and

only granting access to the audio data by the software driver.

17. The non-transitory computer readable medium of claim **13**, further comprising instructions for:

instructing the software driver to grant access to the audio data if the software application requesting access to the audio data is determined as an authorized software application;

processing, by the software driver, the audio data as an audio stream; and

transmitting, by the software driver, the audio data to the determined authorized software application.

18. The non-transitory computer readable medium of claim **13**, further comprising instructions for:

installing, in the memory, a plurality of software drivers associated respectively with a plurality of audio streams of the audio session, the software drivers being configured to prevent access to the audio streams, respectively, by the unauthorized software applications;

receiving process identifier data from at least one software application requesting to access one of the plurality of audio streams;

determining whether the at least one software application requesting access to the audio stream is an unauthorized software application; and

controlling the respective software driver to prevent access to the audio stream by the determined unauthorized software application.

* * * * *